AMENDMENTS TO THE SPECIFICATION

Please amend the specification as indicated below. The language being added is underlined ("__") and the language being deleted contains a strikethrough ("—").

Abstract:

A method and system is provided for generating pseudo-random numbers utilizing techniques of both the SHA-1 and DES encryption standards, wherein a pseudo-random number generator is re-keyed periodically using an external input of physical randomness. In accordance with one embodiment of the present invention, a current seed value S_j is loaded from a non-volatile storage. Next, values E, representative of environmental randomness, and C, representative of configuration data are likewise loaded. A new seed value, S_{j+1}, is generated in accordance with the equation $S_{j+1}=f(S_j; A; C; E)$, wherein f represents a selected encryption algorithm, and AB is a first~~second~~ constant, and wherein S_j is concatenated with A, which is concatenated with C which is concatenated with E. The new seed is then written to the non-volatile storage. Next, a key, K, is generated in accordance with the equation $K=f(S_j; B; C; E)$, wherein B is a second constant. Lastly, a pseudo-random number output, P_n, is generated in accordance with the equation $P_n=f_{3DES}(K, P_{n-1})$, where f_{3DES} represents the operation of triple DES encryption hardware, and P_{n-1} is the previously generated pseudo-random number.

Paragraph [0008]:

[0008] In accordance with one embodiment of the present invention a current seed value S_j is loaded from a non-volatile storage. Next, values E, representative of environmental randomness, and C, representative of configuration data are likewise loaded. A new seed value, S_{j+1}, is generated in accordance with the equation $S_{j+1}=f(S_j; A; C; E)$, wherein f represents a selected encryption algorithm, and ~~AB~~ is a first~~second~~ constant, and wherein S_j is concatenated with A, which is concatenated with C which is concatenated with E. The new seed is then written to the non-volatile storage. Next, a key, K, is generated in accordance with the equation $K=f(S_j; B; C; E)$, wherein B is a second constant. A pseudo-random number output, P_n, is then generated in accordance with the equation $P_n=f_{3DES}(K, P_{n-1})$, where f_{3DES} represents the operation of triple DES encryption hardware, and P_{n-1} is the previously generated pseudo-random number.

Paragraph [0013]:

[0013] Where, the initial value P_0 can be set to any fixed value such as 0. This will provide a source of pseudorandom numbers with a rate of about 15 Mbit/sec. The key K will be derived from a seed S kept externally in non-volatile memory. Initially, on power-up, the device loads the current value S_j of the seed, plus configuration data C and environmental randomness E in step 100. The device will compute the key K in step 104~~102~~ and the next value S_{j+1} of the seed in step 102~~104~~ as follows, using, in one embodiment, the FIPS 180 secure hash standard algorithm (SHA). The seed S_j will preferably be 160 bits in length if the current secure hash standard algorithm SHA-1 is used, and 256 bits if the proposed new standard SHA-256 algorithm is used: